



其他



中信國際電訊集團有限公司 | www.citictel.com

「簡言之，成績超乎理想。中信國際電訊CPC的TrustCSI™託管式安全服務能透過關聯分析，精簡90%無風險記錄，警報時間更縮短至15分鐘內，較我們的理想還要優勝一倍！」

葉漢忠

副總裁

工程及資訊科技部

 **中信國際電訊**
CITIC TELECOM INTERNATIONAL

中信國際電訊著重信息安全確保優質服務 中信國際電訊CPC TrustCSI™託管式安全服務(MSS)， 大幅提升網絡安全水平和穩定性，確保中信國際電訊集團優質的電信服務

中信國際電訊集團有限公司於1999年成立，目前在香港聯合交易所主版上市，股份代號1883。中信國際電訊在亞太地區提供語音服務、移動短信服務和其它增值電信服務（信令轉接、預付費漫遊等）、數據服務和為電信運營商、移動運營商以及互聯網服務商提供電信業務解決方案。

電訊服務公司的信息安全挑戰

近年來，IP網絡交通不斷上升，隨著各式IP應用如IP話音（VoIP）冒起，客戶倚重網絡日深。作為一家電訊服務上市公司，中信國際電訊十分著重網絡的安全和穩定性，故裝置了多重保護如防火牆、防入侵偵察(IDS)/入侵防禦(IPS)系統、防病毒軟件、防垃圾電郵等程式，嚴防惡意入侵。

中信國際電訊集團有限公司增值服務工程及資訊科技部高級經理葉漢忠表示，由於安全問題複雜，因此公司未必能全面掌握漏洞，以致駭客有機可乘，入侵網絡發動惡意破壞。對他們而言，這絕對不能接受。另外，作為大中華區領先的國際電信樞紐運營商，他們致力提供優越的服務，明白網絡一旦被惡意入侵，服務受阻甚至中斷，會大大影響客戶的商業運作及其信心。

只是網上攻擊層出不窮，各安全裝置每天產生的數據，單原始記錄便接近一百萬條。雖然他們早已委專業的網絡工程師每天跟進，然而卻難保沒有漏網之魚。

理想中的安全方案

畢竟人手監察，即使負責者經驗豐富，質素仍難以保證持久穩定。根據葉的經驗，縱使加派人手多重監察，假如在技術和流程上沒有加以配套，始終難以確保萬無一失。

加上人手監察發現問題需時，因此他們便四出尋找不同託管式安全服務，務求將各式安全裝置的原始記錄進行關聯分析，期待能去掉80%無風險數據。並過濾已知屬正常記錄，減少誤警。以及將安全警報時間，由人手的每天24小時檢查一次提升至事故發現半小時之內，防止事態蔓延。

你最可信賴的信息技術方案伙伴



TrustCSI™一系列託管式安全解決方案，由擁有安全認證的專家團隊管理，配合中信國際電訊CPC安全運作中心(SOC)24x7全天候的監察，針對不斷湧現的網絡威脅，為企業提供業務獨特需要而設的解決方案。



預防



修正



偵測

為此葉等四出查詢不同方案，包括中信國際電訊CPC提供的TrustCSI™託管式安全服務，並發現其服務最為全面，並可按其需要作顧客化制定。而且其他相似服務組合，較TrustCSI™甚至昂貴達30%，因此決定採用。

中信國際電訊CPC TrustCSI™信息安全效益超乎理想

現時中信國際電訊CPC為中信國際電訊網絡的防火牆、IDS/IPS系統及防病毒裝置提供TrustCSI™託管式安全服務，結果：

- 成功透過關聯分析，剔除多達90%無風險記錄
- 過濾預設的安全事件，減低誤警
- 縮短警報時間，由原先協議的30分鐘提升至約15分鐘

葉表示：「簡言之，成績超乎理想。我們最初期望中信國際電訊CPC的TrustCSI™託管式安全服務能透過關聯分析，削去80%的無風險記錄，以及將警報周期由過去的每天檢查縮短至30分鐘內。結果他們的關聯分析能精簡90%無風險記錄，警報時間更縮短至15分鐘內，較我們的理想還要優勝一倍！」

葉續表示：「我們現已不用委派專人每日跟進安全事態記錄，而是由輪班工作的緊急服務人員，隨時跟進有關的事件警報。曾經，我們因為知道一些警報是由於系統維修做成，故此，我們沒有按程序處理警報，也沒有臨時啟動過濾，結果TrustCSI™不斷示警，以致中信國際電訊CPC的信息安全專家來電跟進。從中可看到他們認真的專業態度。」

更令葉意外的，是由中信國際電訊CPC提交的每月安全報告，附上每部伺服器及安全裝置的分析數據，讓他們察覺到一些過

去在網絡管理記錄上隱而未顯的非正常現象，令他們提高警覺，並針對深入剖析，研究背後原因，或相應增加頻寬，有利他們的長期規劃。

技術、流程、專家鐵三角組合

葉相信，單憑人手無法完全處理安全問題，因為人的一些習性，例如容易忽略反覆出現的事件，形成狼來了心態，降低警覺。遇到不正常現象時，傾向尋找簡單解析，缺少主動發掘透徹了解問題。因此，除了中信國際電訊CPC擁有的安全專家，他更欣賞TrustCSI™託管式服務先進的關聯和安全信息及事件管理(SIEM)技術，能客觀地偵察所有的潛在安全事件，以及事件處理機制，讓他們可快速地作出最合適的對應行動，阻截問題發生。

中信國際電訊CPC的安全專家通過各種國際安全認證，包括CISA、CISSP以及SecurityPlus。中信國際電訊CPC的安全運作中心(SOC)同時獲ISO9001及ISO27001優質管理認證，並遵行以IT基建資料庫(ITIL)為本的處理程序，擁有強力的安全信息及事件管理(SIEM)技術，透過專業人才、先進技術、標準程序三結合，滿足中信國際電訊集團有限公司最嚴謹專業的要求。

在服務應用第一階段，葉已將最關鍵的IDS/IPS系統先行移交TrustCSI™ MSS。預算經一年合約應用後，再總結經驗及分析公司的實際需要，作進一步合作部署其他安全方案，以應付日益猖獗的網上威脅。

中信國際電訊CPC

- W: www.citictel-cpc.com
- 亞太區: info@citictel-cpc.com
- 歐洲及CIS: info-eu@citictel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
俄羅斯 T: 7 495 981 5676

台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30
荷蘭 T: 31 20 567 2000

中國大陸 (Toll Free): 400 651 7550
新加坡 T: 65 6220 6606